==Phrack Inc.==

Volume 0x0e, Issue 0x44, Phile #0x10 of 0x13

Lines in the Sand: Which Side Are You On in the Hacker Class War

by Anonymous

With dramatically growing hacker and leaker activity paralleling the revolutionary upheavals around the world, we are increasingly hearing the rhetoric of "cyberwar" thrown around by governments attempting to maintain legitimacy and exercise more police-state powers. In talking about the FBI's priorities ten years after 9/11, FBI director Robert Mueller stated in a recent speech at the International Association of Chiefs of Police(IACP) conference that "the next threat will be cyber-based ... self-radicalized individuals using online resources and individuals planning cyber attacks" [21]. Although hackers made a mockery of Mueller and the IACP during the conference by defacing their websites, it is hard to believe that hackers are a bigger threat than the "terrorists". Still, this logic is being used to send many more billions of dollars into white hat pockets at private military and intelligence contracted corporations to develop better defensive and offensive technology. The US is also proposing several changes to the 1986 Computer Fraud and Abuse Act, providing increased sentences (including mandantory minimums) as well as RICO Act classifications for computer hacking. For the most part, the increased hacker busts have largely targeted small-time defacers and DDoS kids allegedly affiliated with Anonymous - hardly the "foreign terrorist threat to critical infrastructure" used to justify the proposed increased penalties for hackers and increased cashflow to the security industry. But there's more than small timers at play: attacks against high profile institutions including law enforcement, military and corporate targets have escalated, becoming both more destructive as well as more politically articulate. We're experiencing the opening stages of the next Hacker Class War, and with many factions at play each operating with their own agenda and strategies, with more and more hackers breaking into shit for the rev or selling out to the military intelligence industrial complex, the question is asked "which side are you on"?

U.S. military officials, eager to talk about how the Pentagon has boosted its computer defenses, often remain quiet when asked about its offensive Internet capabilities. A list of cyber capabilities-- available only to policymakers-- is described as ranging from planting a computer virus to bringing down electric grids [1]. This would not be possible if it were not for the assistance of computer hackers working directly or indirectly for the Department of Defense, as well as the tendency in our communities to support or tolerate those who choose to do so. Unfortunately, this mentality is frequently espoused by figureheads commonly quoted in mainstream news articles, where they claim to speak on behalf of the hacker community. Conversely, there has always been resentment from black hats and the criminally minded for the corporate sellouts who claim to be hackers but instead choose to protect systems against those who actually break into them. Much has been written about the corrupt white hats who work to protect vital infrastructure against other, more fun-loving hackers. Many lulz have been had over the years every time these big shots get owned and all of their emails and passwords are released in nicely formatted .txt

files. Besides FBI collaborating fucks and security "professionals", it is time to call out the other emerging threat to the integrity of our scene: the US military's active effort to train and recruit hackers into aiding US cyber "defense" systems.

With the passage of the 2012 Defense Authorization bill, the DoD has "express authority to conduct clandestine military activities in cyberspace in support of military operations". Reuters reports that "the Pentagon has put together a classified list of its offensive cyber capabilities so policymakers know their option". To what extent the US has already engaged in offensive electronic attacks is for the most part speculative. It is widely speculated that the US or Israeli military, or both cooperating, developed STUXNET to destroy Iran's nuclear facilities [2].

To fill the need for skilled security people, the military operates several schools and training classes designed to turn young enlisted computer enthusiasts into skilled hackers. The US Military Academy in West Point, NY has an ACM SIGSAC chapter which teaches special classes on remote intrusion techniques and periodically hosts several live hacking competitions to "train and engage enlisted military, officer, or government-affiliated civilians". Last April, the West Point team was victorious over "veteran hackers from the NSA" at the 2011 Cyber Defense Exercise. Other military hacker teams such as ddtek (as led by Lt. Cmdr Chris Eagle who regularly speaks at DEFCON and Blackhat) also compete in civilian hacker tournaments such as DEFCON's CTF, usually dominating the competition by bringing dozens of Navy cybersecurity graduates [3][4]. No doubt many of these people will eventually be working at USCYBERCOM or other clandestine military hacker operations to launch attacks on behalf of the rich ruling class.

The US government must not have too much faith in their enlisted hackers, because they collaborate with a variety of private companies and individuals to defend their networks as well as profiling, infiltrating and attacking their enemies. After LulzSec owned and leaked emails for the CEO of military-contracted security firm Unveillance and Infragard member Karim Hijazi, he was exposed to have been working with the DoD and the White House to not only profile "main hacking groups in Libya and their supporters" but also take the offensive and "map out Libya's Oil companies and their SCADA system's vulnerabilities" [5]. Even after Karim was owned and exposed he was willing to pay cash and offer his botnet to LulzSec to destroy his competitors, further revealing the white hat's corrupt and backstabbing nature as well as revealing how desperate and vulnerable the most powerful military in the world really is.

Then there's Aaron Barr, the former CEO of HBGary Federal, who was served with swift and fierce justice-- being exposed for engaging in counter-intelligence operations attempting to disrupt both WikiLeaks (where he suggests "cyber attacks against the infrastructure to get data on document submitters") and Anonymous (where he cooperated with the FBI attempting to profile "key leaders") [6]. The leaked emails also reveal a bid to develop "persona management software" for the US military which is another COINTELPRO-type tool to spread propaganda by creating an army of fake twitter, facebook, blog, forum accounts to subvert democracy and manipulate public opinion. Although Barr/HBGary and Karim/Unveillance/Infragard have been exposed and humiliated, the implications of what has been released involving their work demonstrate a frightening and possibly illegal conspiracy between private security corporations collaborating with government and military to silence and disrupt their political opponents.

Despite the obvious failures of their affiliates, the military continues to try to draw talent from independent hackers. DARPA made a public offering

to hackerspaces in the US to do "research designed to help give the U.S. government tools needed to protect against cyberattacks". The program Cyber-Insider (CINDER) is headed by Peiter "Mudge" Zatko [7] who-- like many of us-- used to be a teenage hacker associated with the Cult of the Dead Cow and old-school hacker space l0pht. Peiter eventually "went straight" when they formed security consulting firm @Stake which was later acquired by Symantec. Now he's completed the vicious circle from teenage hacker to "security professional" to full blown military employment, serving as an example to aspiring hackers as what NOT to do. Mudge has now been speaking at hacker conferences like Schmoocon as well as various DARPA Industry Day events in an attempt to recruit more hackers into the DARPA fold. Hackerspaces, which are becoming a growing trend not only in the US but also internationally, are often strapped for cash to pay rent or purchase equipment, and because of unique problem-solving skills and a DIY hacker ethic are being looked at by employers in both private and government fields. Unfortunately, many hackerspaces are "non-political" and are mostly composed of people more interested in a career than the hacker ethic, making many especially vulnerable to pressure to do research for the military or inform on other hackers to law enforcement.

Hackerspaces aren't unique for being wishy-washy and apathetic in this regard: hackers in the US have a long history of big names going federal. Adrian Lamo, once known as the "homeless hacker" after turning himself in for breaking into several high profile news websites, is now universally hated as the dirty snitch who turned in alleged WikiLeaks leaker Bradley Manning. Despite this, Adrian still openly affiliates with 2600-- running their facebook group, making occasional appearances on IRC, and most recently being invited to speak on a panel at the 2010 HOPE convention. Then there's Kevin Mitnick-- whose social engineering skills somehow qualify him as some sort of spokesperson for hackers-- who has resigned himself (like so many others) to the "industry" doing professional security consulting and making big bucks giving speeches and signing books at conferences (and like so many others he has become a target of black hats who have repeatedly owned his servers and released his private emails and passwords) Jeff "The Dark Tangent" Moss, who for more than a decade headed the "largest underground hacking convention" DEFCON and the grossly-misnamed Black Hat Briefings ended up working for the Department of Homeland Security. Then Oxblood Ruffin from the "underground" group Cult of the Dead Cow (which was also owned hard by black hats) runs his mouth on Twitter claiming "ownership" of the term "hacktivism" while repeatedly denouncing other hackers(specifically "black hats" and "anonymous") who break into and attack systems, going so far as to sign a joint statement by cDc, 2600, l0pht, CCC and others condemning Legion Of The Underground's attacks against the Iraqi government for human and civil rights abuses [8].

Another more recent example of treachory in the hacker community is the case of 'security consultant' Thomas Ryan (aka frogman) who infiltrated and released internal mailing list communications for the NYC Occupy Wallstreet protesters. For months he worked his way in, gaining access and trust, while at the same time forwarding protest plans to the FBI and several news organizations, eventually dumping everything to right-winger Andrew Breitbart's website as "proof" of "illegal anarchist activities". In the same files he released he accidentally included his own correspondence with the FBI and news organizations (some "security professional"). Thomas Ryan's white hat and right-wing leanings were rather well known in hacker circles, as well as his social engineering exploits (he previously spoke at the "black hat briefings" about his experiences tricking dozens of government employees and security cleared professionals by using a fake profile of an attractive and skilled woman named "Robin Sage": unfortunately he did not dump any private or embarassing information on his white hat brethren). Certainly the primary point of failure for OWS was

poor security culture, trusting an already well-known reactionary white hat to their internal communications and protest details (a weakness of an open-source movement as opposed to closed private collectives composed of vouched-in members). However when this betrayal falls from our own hacker tree, we need to take responsibility and discourage future treachory (like how Aaron Barr was served by Anonymous).

Then there's 2600 which is composed of several separate communities including the local meetups, the magazine, Off The Hook, and the IRC community. To be fair, Eric Corley is somewhat friendly to the interests of hackers, supporting digital rights, criticizing the police state, and being generally left-leaning. But upon closer inspection you'll find a very disturbing militaristic anti-wikileaks, anti-EFF and straight up anti-hacker mentality held by many of the people involved: half the ops on 2600net have no problem openly bragging about working for the military or collaborating with law enforcement. Just like ten years ago in their condemnation of LoU, 2600 released a statement in December condemning Anonymous ddos attacks against the banks and credit card corporations that were ripping off WikiLeaks [9] (a tactic that is nothing more than a digital version of a sit-in, a respected tradition of civil disobedience in US politics). Using the 2600 name to condemn Anonymous actions not only undermines our work but creates the false impression that the hacker community does not support actions against PayPal in support of Wikileaks. More than six months later, the FBI carried out raids at the homes of several dozen alleged Anonymous "members" who were purportedly involved with carrying out the LOIC attacks against PayPal. In light of how dozens of people (who may not even have been involved at all) may be facing decades in prison for some bogus trumped up federal conspiracy charges, what kind of credibility should be given to 2600 who clearly has no regard for practicing solidarity with hackers facing unjust persecution?

The 2600net IRC network itself is run by a DoD-cleared, Infragard-trained "r0d3nt" named Andrew Strutt who works for a military-contracted company and has in the past openly admitted to working with law enforcement to bust people he claims were running botnets and distributing child porn. Andrew Strutt's interview for GovExec.com [10] read: "'I've had to work hard to build up trust,' Strutt adds that he doesn't disclose his identity as a hacker to the people he refers to as his handlers. And he doesn't advertise to hackers that he works for the .mil or .gov community either". Most recently, r0d3nt voluntarily complied with a grand jury subpoena where he gave up the shell server "pinky" to the feds and kept quiet about it for months [11]. The shell server had several hundred accounts from other members of the 2600 community who now have the displeasure of knowing that law enforcement forensics are going through all their files and .bash_history logs. Strutt kept this a secret from everybody for months (complying with a clearly illegal "gag order") and has since been very vague about details, refusing to answer questions as to the specifics of the investigation except that law enforcement was looking for "a certain user"'s activity on the box. Of course it is reckless and stupid to use a community shell server to carry out attacks putting other users on the box in danger, but this is something you should be prepared for well ahead of time if you put yourself in such a place. Many ISPs that host websites and listservs for radicals and hackers not only have a clearly defined privacy policy reducing the amount of personally identifiable information on the box, but also have a "will not comply" statement that says they will never voluntarily give up the box. This was demonstrated in November 2009 where IndyMedia.us received a similar gag order and subpoena asking for log files on the server (which never existed in the first place). The folks there immediately got the EFF involved and publicly announced the government's unjust fishing expedition, saying they had no plans on complying. In the end, nothing was given up and the gag order was found to be

unconstitutional [12].

Why do many of the big name hackers that are seen as role models end up being feds and corporate sellouts, and why are these people still welcomed and tolerated in the scene? Eric Corley of 2600 estimated that a quarter of hackers in the US are FBI informants [13], which is unfortunately an astonishingly high figure compared to other fields. Experienced criminals who have done prison time will tell you that the code of the street is don't trust anybody and don't rat. If you ask many younger hackers, they'll casually joke about breaking into systems in their youth but if they ever grow up or get busted they'll be working for the government. Dealing with the devil never ends up well for anyone involved: all they want to do is bust other hackers, and in the end after using and abusing their informants they often kick them to the curb.

Albert Gonzales (aka "soupnazi", "cumbajohnny", and "segvec") became an informant after he was busted in NYC for credit card fraud and was paid $75,000 to infiltrate carding websites like ShadowCrew. Despite his cooperation with the Secret Service where he sent several dozen hackers and fraudsters to prison as part of Operation Firewall, the feds STILL indicted Gonzales on some fresh credit card fraud charges of his own and sent his rat ass away for several decades. Unfortunately one of the people roped into Gonzales' web of deception was the notorious black hat Stephen Watt "the unix terrorist" who helped write old school zines like el8 and left a trail of mail spools, ownage logs, and rm'd servers of the most respected "security professionals" in the industry. Watt was never even charged with participating in any of Gonzales' money schemes but simply wrote some common packet sniffing code called 'blabla' which was supposedly used to help intercept credit card transactions in TJX's networks, demonstrating how depraved and desperate the feds are to make quotas and inflate the threat of hacker fraud artists in the media [14].

While many support our fallen hacker comrades like the Unix Terrorist, we still hear a startling line of thought coming out of the infosec community. Ask around at your 2600 meeting or hackerspace and you'll hear a condemnation of imprisoned hackers as being nothing more than criminals along with a monologue comparable to politicians, police officers and the media: don't break into other people's systems, don't ddos, don't drop dox and if you find a vulnerability, "please please report it to the vendor so it could be patched." To think this mentality is being perpetuated by people who wave the hacker flag is disgusting and undermines the work that many legit hackers have fought and went to prison for.

Because so many who claim to represent hackers end up working for the very corrupt and oppressive institutions that other hackers are fighting against, it is time to draw lines in the sand. If you are military, law enforcement or informant, work for a DOD contracted company or a private security firm hired to bust other hackers or protect the infrastructure we aim to destroy, you are no comrade of ours. This is 2011, the year of leaks and revolutions, and every day we hear about riots around the world, and how major corporations and government systems are getting owned by hackers. The papers have been describing recent events as a "cyberwar" (or more accurately, a "hacker class war") and the way the attacks have become more frequent and more damaging, this is not much of an exaggeration.

It is impossible to talk about contemporary hacktivism without mentioning Anonymous, LulzSec and Antisec. Responsible for dramatically raising the stakes of this "war," they have adopted an increasingly explicit anti-government and anti-capitalist stance. The decentralized model in which Anonymous operates parallels every successful guerrilla warfare campaign waged throughout revolutionary history. In just a few months, they

have taken aim at the CIA, the United States Senate, Infragard, Sony, NATO, AT&T, Viacom, Universal, IRCFederal, Booz Allen, Vanguard Defense Industries, as well as Texas, Missouri, Alabama, Arizona, Boston, and other police departments -- dropping massive username/password lists, confidential law enforcement documents, personal email correspondence and more. The latest campaign -- "Operation Antisecurity" -- is designed to unite other hacker groups, tipping their hats to old school antisec days while bringing more attention to anti-government black hat politics as has never before seen [15]. Although the attack methods being utilized have been relatively primitive-- ranging from common web application vulnerabilities like RFI/LFI and SQL injection, to brute force DDOS and botnet attacks-- there are signs that their attack methodology is becoming more sophisticated, especially as talent from allied hacker crews becomes involved. Additionally choice of targets are going after our bigger enemies: while past incarnations of antisec have humiliated many well-known sellouts in the computer security industry, today's blackhats are not scared to hit higher profile figures in law enforcement, military, and governments most notably by mercilessly dropping usernames, passwords, home addresses and phones, and social security numbers to tens of thousands of police and military officials.

As hackers continue to expose and attack corruption, law enforcement will desperately continue to try to make high-profile arrests regardless of actual guilt or association. Especially as politicians continue to try to classify hacktivism as an act of cyber-terrorism (which can be retaliated against as traditional acts of war [16]), the threat of prison is very real and people should be well prepared ahead of time for all possible repercussions for their involvement. We should not, however, let the fear of government repression scare us into not taking action; instead, we should strengthen our movement by practicing better security culture and working to support other hackers who get busted in the line of duty. Even though there are plenty of guides out there on how to become "anonymous", many mistakes have already been made: trusting the mentally unstable 19 year old Ryan Cleary to run the LulzSec IRC server, for example. Even before he was actively cooperating with the feds after being arrested in a joint US-UK operation, Ryan was already known to double-cross other hackers, having posted IP information of hundreds of anonops IRC users [17][18]. Although it's righteous to out snitches and movement traitors to the public, doxing other hackers involved in the struggle is only making law enforcement's job easier to identify and prosecute our comrades. Now more than ever should folks unite and practice solidarity with each other, setting aside our differences to go after our common enemies.

The events over the past few months have been compared to the glory days of the 90s, complete with IRC wars and major website defacements. As breaking into computer systems becomes popularized and a new batch of young bloods are emerging on the scene, many questions remain. Is government going to make more arrests and pass more draconian laws? Would they be doing the same thing anyway-- even if hackers weren't striking back? Is Anonymous actually damaging the white-hat military and intelligence security industries with the ownings, defacements, and leaks, or are they just bringing heat on the underground while providing justification for more government financing of our enemies? Is this just another script kiddie scene thriving on sqlmap and milw0rm exploits or is there old school talent behind the scenes owning shit to keep the antisec flame alive? Most importantly, how can those fighting the hacker class war better coordinate their work with street-level resistance movements?

As attacks intensify, no doubt governments will try to put more money into defending their infrastructure, holding more internal security trainings, and passing more laws increasing penalties for computer hacking as well as

censoring and invading our privacy. The government propaganda machine will no doubt blame hackers as some sort of cyber-Al Queda to demonstrate the need for heightened security. Don't get it twisted: they have always wanted to pass these laws in the first place and would have done so with or without using the hacker threat as scapegoat, just as they wanted to go invade Afghanistan and Iraq and pass the PATRIOT Act before 9/11 ever happened. Don't be scared by ridiculous statements like FBI deputy assistance Steven Chabinsky who announced regarding the anonymous PayPal arrests, "We want to send a message that chaos on the Internet is unacceptable, [even if] hackers can be believed to have social causes, it's entirely unacceptable to break into websites and commit unlawful acts". Yes, the feds will continue to paint us as terrorists whether we act or not and will continue to make sweeping arrests regardless of guilt or innocence in an attempt to demonstrate that they aren't losing the cyberwar after all when all signs show that they are. It's widely speculated that the unexpected resignation of US-CERT director Randy Vickers is related to the dramatic increase in high-profile internet attacks against government institutions [20].

Another sign of success is how the threat of being targeted by Anonymous and other anti-censorship activists could possibly scare the companies into not going forward with their plans, which is exactly what happened to Australian ISP Telstra [20]. A practice that seems to have been revived from old school black hat days is the targeting of security professionals and hackers who choose to sell out and work for corporations and governments to protect their systems. This is an effective strategy because not only are they ridiculously incompetent and corrupt low-hanging fruit, but they likely hold private information on the cyberwar activities of the military. Additionally, hitting them hard and repeatedly will serve as a warning to others who would follow their lead and sell out their skills to the enemy: think twice before you find yourself in the crosshairs. What would happen when the government invests all this money to hire more hackers to protect their systems, but no one showed up?

Hackers may brag about their antics instantly getting international news coverage but the offensive cyber operations of the US military are considerably quieter. Not only does this keep their enemies from knowing their capabilities but also because much of the work being done is likely illegal. As the saying goes, those who make the laws are allowed to break them. When teenagers hack into high profile systems, they're considered criminals and even terrorists; the governments and militaries of the world do the same at greater magnitudes while hiding behind the guises of national security or "spreading democracy." It might be a while before we ever hear about some of the operations hackers working for the military are involved in. Then again, it might not-- maybe they'll be the next ones owned, having their private data plastered all over the Internet.

---

[1] "President lays out cyberwar guidelines, report says"
http://news.cnet.com/8301-13506_3-20073314-17/president-lays-out-cyberwar-guidelines-report-says/

[2] "Stuxnet apparently as effective as a military strike"
http://arstechnica.com/tech-policy/news/2010/12/stuxnet-apparently-as-effective-as-a-military-strike.ars

[3] "Eagle Soars to Top of NPS"
http://www.navy.mil/search/display.asp?story_id=2886

[4] "Poke in the Eye to SANS and CISSPs in Defcon 18 CTF Announcement"

http://sharpesecurity.blogspot.com/2010/04/poke-in-eye-to-sans-and-cissps-in.html

[5] "Fuck FBI Friday Pretentious Press Statement"
http://LulzSecurity.com/releases/fuck_fbi_friday_PRETENTIOUS%20PRESS%20STATEMENT.txt

[6] "How One Man Tracked Down Anonymous And Paid a Heavy Price"
http://www.wired.com/threatlevel/2011/02/anonymous/all/1

[7] "Hacker 'Mudge' Gets DARPA Job"
http://news.cnet.com/8301-27080_3-10450552-245.html

[8] "Joint Statement Condemning LOU Cyberwar"
http://www.2600.com/news/view/article/361

[9] "Press Release - 2600 Magazine Condemns Denial of Service Attacks"
http://www.2600.com/news/view/article/12037

[10] "Hiring Hackers"
http://www.govexec.com/features/1110-01/1110-01s1.htm

[11] "Statement regarding Seizure of pinky.ratman.org shell server."
http://foster.stonedcoder.org/~r0d3nt/statement.txt

[12] "From EFF's Secret Files: Anatomy of a Bogus Subpoena"
https://www.eff.org/wp/anatomy-bogus-subpoena-indymedia

[13] "One in Four Hackers in the U.S. is an FBI Informant"
http://publicintelligence.net/one-in-four-hackers-in-the-u-s-is-an-fbi-informant

[14] "TJX Hacker Was Awash in Cash; His Penniless Coder Faces Prison"
http://www.wired.com/threatlevel/2009/06/watt/

[15] "50 Days of Mayhem: How LulzSec Changed Hacktivism Forever"
http://www.pcmag.com/article2/0,2817,2387716,00.asp

[16] "Pentagon to Consider Cyberattacks Acts of War"
http://www.nytimes.com/2011/06/01/us/politics/01cyber.html

[17] "Teenage 'Cyber Hacker' Son is Accused of Bringing Down 'British FBI' Site"
http://www.dailymail.co.uk/news/article-2007345/Ryan-Cleary-Hacker-accused-bringing-British-FBI-site.html

[18] "LOL ANONOPS DEAD"
https://sites.google.com/site/lolanonopsdead/

[19]"Agency Chief Tasked With Protecting Government Networks From Cyber Attacks Resigns"
http://www.huffingtonpost.com/2011/07/25/chief-protecting-government-networks-resigns_n_909116.html

[20] "Anonymous and LulzSecs Existence Scares ISP into Halting Web Censorship"
http://www.zeropaid.com/news/93950/anonymous-and-LulzSecs-existence-scares-isp-into-halting-web-censorship/

[21] "FBI Director Mueller Explains FBI Priorities 10 Years after 9/11"
http://theiacpblog.org/2011/10/25/fbi-director-mueller-explains-fbi-

priorities-10-years-after-911/

[EOF]